REMARKS

Reconsideration of this application is respectfully requested in view of the foregoing amendments and the following remarks. Claims 31-51, 53-79, and 81-84 are pending, with claims 31, 47, 62, 69, and 76 being the independent claims. Based on the foregoing amendments and the following Remarks, the Applicant respectfully requests that the Examiner reconsider and withdraw all outstanding rejections.

Interview Summary

The undersigned appreciates the time and attention extended by Examiners Jakovac and Swearingen during the telephone interview conducted on February 23, 2008. During the interview, the participants discussed the state of the prior art.

Claim Rejections Under 35 U.S.C. § 102(b)

Claims 31-51, 53-79, and 81-84 were rejected under 35 U.S.C. § 102(b) as being anticipated by WO 01/10090 to Tomkow ("*Tomkow*"). Applicant respectfully submits that none of the independent claims, as amended, are anticipated by *Tomkow*.

Tomkow discloses a system and method for secure and tamper-proof documentation of the content and delivery of an electronic message, such as an e-mail. In *Tomkow*'s method, an "originator" sends to the "RPost server" 14 a message addressed to a "message recipient" 18.

The RPost server first preprocesses the message. The preprocessing includes:

- creating database records to store information about the message and each destination for the message, including the "Delivery Status";
- performing hashing functions on the message's contents;
- storing a copy of the original message and its attachments; and
- adding headers to the message requesting a read notification from each message recipient's MUA/MTA.

Tomkow pp. 10-17

The RPost server then transmits the modified message to each message recipient's MUA/MTA. *Tomkow* pp. 17-20.

Finally, the RPost server performs "postprocessing" on the message. This includes:

- processing and saving Delivery Status Notifications (DSNs) from the message recipient's MTA
- creating a "delivery receipt" 20 for the message, in the form of an e-mail sent to the original sender of the message. The delivery receipt includes, among other components:
  - the body of the original message,
  - a list of the original attachments to the message, with separate message digests of each attachment; and
  - copies of the original attachments.

  Each of the elements of the delivery receipt may have message digests or digital signatures included in the receipt, and the receipt may include a single overall encrypted message digest or digital signature appended as part of the receipt.
- sending the delivery receipt to the original sender of the registered message; and
- expunge all records of any data concerning the message or its delivery.

Tomkow pp. 20- 25.

When the originator of a message requires evidence that an e-mail was sent, delivered, and/or read, the originator presents the receipt(s) for the message to the RPost server. The RPost server determines whether or not the receipt is valid:

> A receipt is valid if the digital signature matches the remainder of the receipt, and the message digests match the corresponding respective portions of the original message. Specifically, RPost performs the hash function on the various portions of the message . . . to produce one or more message digests corresponding to the purported message copy. RPost compares the message digests in the purported copy, including the overall message digest, with the message digests which RPost has computed from the purported message copy. . . . If the message digests including the digital signature match, then the receipt is an authentic RPost-generated receipt.
>
> *Tomkow*, pg. 26.

In contrast, the claimed system and methods are directed to determining whether or not a message was authorized by a purported originator of the message. Each of claims 31 and 47 (as amended) recite:

> receiving on behalf of the intended recipient a confirmation request including said identification data and requesting confirmation that said electronic message was authorized by the originator; and
>
> comparing said identification data received in said confirmation request to said stored identification data.

Similarly, each of clams 62 and 69 (as amended) recite

> receiving a confirmation request to confirm that an electronic message sent to an intended recipient was authorized by an originator identified in the electronic message, the confirmation request including identification data purporting to uniquely identify the electronic message;
>
> searching a data store, separate from said electronic message, for said identification data

Applicants understand the Examiner to assert that the claimed "confirmation request" can be read onto *Tomkow*'s delivery receipt, and that the claimed comparison of identification data in the information request to the stored identification data can be read onto *Tomkow*'s verification of the delivery receipt. Applicant respectfully submits that this reading is erroneous, and has amended these portions of the claims to more clearly recite that the confirmation request is made on behalf of the intended recipient of the message, to request confirmation that the message was authorized by the originator of the message, and that the comparison is to identification data that is stored separately from the electronic message. As summarized above, *Tomkow* is concerned with verification of the validity of a receipt evidencing that a message was delivered to a recipient, and explicitly teaches that no information about the delivery receipt is stored by the RPost server – rather, the server simply verifies the message digest(s) and digital signature(s) by executing the same hash / signature algorithm(s) on the message content that is included within the delivery receipt, which is provided back to the RPost server by the originator of the message. *Tomkow* thus does not anticipate any of independent claims 31, 47, 62, or 69 (or any of their dependent claims 32-46, 48-51, 53-61, 63-68, or 69-75), and Applicant respectfully submits that the claims are allowable.

Claim 76 (as amended) recites:

> sending to a confirmation device a first confirmation request requesting confirmation that said first electronic message was authorized by the originator;
>
> sending to the confirmation device a second confirmation request requesting confirmation that said second electronic message was authorized by the originator.

Applicant respectfully submits that *Tomkow* does not disclose sending to a confirmation device first and second confirmation requests, each of which requests confirmation that respective first and second electronic messages were authorized by the originator, and therefore that claim 76 (and claims 77-79 and 81-94 dependent therefrom) are allowable.

Conclusion

In view of the foregoing, Applicants respectfully requests that the Examiner reconsider all outstanding rejections and that such rejections be withdrawn. Applicants believe that a full and complete response has been made to the outstanding office action and thus that the present application is in condition for allowance. If the Examiner believes, for any reason, that further personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 50-1283.

Dated: April 24, 2009

Respectfully submitted,
COOLEY GODWARD KRONISH LLP

COOLEY GODWARD KRONISH LLP
ATTN: Patent Group
777 6th Street NW, Suite 1100
Washington, DC 20001

By:

C. Scott Talbot
Reg. No. 34,262

Tel: (703) 456-8000
Fax: (202) 842-7899

400468 v1/RE